CSS322 – Quiz 6

Name: _____

ID: _____ Mark: _____ (out of 10)

Question 1 [2 marks]

a) What is the difference (in parameters) between a Hash function and a MAC function?

b) What algorithm can used to convert a Hash function into a MAC function?

c) Explain a benefit of converting a Hash function into a MAC function.

Question 2 [5 marks]

a) Assuming users must be allowed to choose any password they wish, describe two different approaches that can be used to make systems more secure against online password guessing attacks. [2 marks]

b) Assuming a user had an 10-character password. Which would you consider the strongest against a dictionary attack?
   i. Random characters
   ii. Combination of two English words
   iii. Pronounceable string (without dictionary words)
   iv. Combination of several names (in English), with mixed upper and lower case.

c) For practical purposes (e.g. efficiency, ease of use), hash functions have three desirable properties. Which of the following is NOT a desirable property of a has function:
   i. Produces fixed length output
   ii. Hard to compute for any input message
   iii. Works on variable sized input messages
   iv. None of the above

d) If you are developing a MySQL database to store customer information for a business, what is the best approach to store the password:
   i. Save it as plain text
   ii. Encrypt the password with Triple-DES
   iii. Hash the password with SHA-256
   iv. Don't store the password in the database, store it as plain text in a separate file

Question 3 [3 marks]

An attacker C intercepts a message, and a signed hash of that message, that was sent from A to B. That is, C intercepts: M || $E(PR_A,H(M))$.

a) If the hash function H() does not have the weak collision resistance property, then can the attacker modify M without B detecting the modification (YES or NO). Explain your answer.

b) If the hash function H() has the weak collision resistance property, but does not have the strong collision resistance property, then can the attacker modify M without B detecting the modification (YES or NO). Explain your answer.